

Robust self-testing quantum states and binary nonlocal XOR games

Carl A. Miller^{1,*} and Yaoyun Shi^{1,†}

¹*Dept. of Electrical Engineering and Computer Science,
University of Michigan, Ann Arbor, MI 48109, USA*

(Dated: July 10, 2012)

Self-testing a quantum state means verifying the existence of a certain multipartite quantum state based only on knowledge of the probability distributions of certain measurements on the state. Self-testing is possible even when the measurement devices are untrusted. This paper is concerned with proving robust (i.e., error-tolerant) self-testing results. We devise a general scheme for proving such results for nonlocal binary XOR games. We apply this scheme to prove a result for the Greenberger-Horne-Zeilinger paradox.

Suppose that two parties, Alice and Bob, share a bipartite quantum state system (Q_A, Q_B) and each possesses a prescribed set of measurements on his or her subsystem. Suppose that the state of the system is not known, but suppose that we know the joint probability distributions of Alice's and Bob's measurement-outcomes for any pair of prescribed measurements. In some cases, this information alone is sufficient to deduce the state of the system (A, B) . If a system of two qubits is such that joint measurements along the x -axis will always agree, and joint measurements along the z -axis always agree, then the state of the system must be the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Taking this idea a step further, we may ask whether we can determine the state of a quantum system based only the outcome distributions of some *unknown* quantum measurements. This is the notion of self-testing of quantum states, and it is possible in some cases. For example, if a collection of binary measurements on a system is known to achieve the optimal quantum violation of the CHSH inequality, then the system must be equivalent to a collection of Φ^+ -pairs [1].

The notion of self-testing of quantum states is crucial for quantum protocols that involve untrusted devices. For example, in the task of randomness expansion from an untrusted device, a party wishes to use an untrusted quantum device to generate random numbers. The party has no knowledge of the inner workings of the device, and can base his trust in the randomness of the device only on its observed classical outputs. Self-testing results for quantum states give the basis for security proofs for such devices. The idea of self-testing in the context of security proofs goes back at least as far as Mayers and Yao in 1998 [2], and it can be seen in more recent work on randomness expansion [3], [4].

In order for self-testing results to be practically useful in randomness expansion protocols, they must tolerate error. It is not sufficient to know that particular measurement-outcome distributions guarantee the existence of a particular state Φ ; we must also know that when the distributions are close to some prescribed distributions, then the underlying state must be close to the

target state Φ .

McKague *et al.* proved that the CHSH paradox is a robust self-test for a Bell state [5]. In independent work, the authors of the present paper proved that the Greenberger-Horne-Zeilinger (GHZ) paradox is a robust self-test for the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ [6]. The purpose of the present paper is to provide a general scheme for proving robust self-testing results which applies to both the GHZ and CHSH games. The scheme builds on the method used in [6].

We work within the class of nonlocal binary XOR games (that is, binary games for which the scoring rule is based only on the XOR of the outputs). We show that if a binary nonlocal XOR game satisfies certain simple criteria—based on the behavior of an associated multivariable sinusoidal function—then it satisfies a robust self-testing result. The criteria that we prove is fairly easy to use provided that the number of parties n is not too large. As a demonstration of the theory, we provide a short proof of a robust self-testing result for the GHZ paradox.

We note that a robust self-testing result for the GHZ paradox was obtained independently in the recent paper [7].

Definitions. For our purposes, a *binary nonlocal XOR game* is simply a function $f: \{0, 1\}^n \rightarrow \mathbb{R}$. The function f describes a scoring rule for the game: if the input sequence is (i_1, i_2, \dots, i_n) , and the output sequence satisfies $\oplus_k o_k = 0$, then the score is $f(i_1, i_2, \dots, i_n)$; if the input sequence is (i_1, i_2, \dots, i_n) and the output sequence satisfies $\oplus_k o_k = 1$, then the score is $-f(i_1, i_2, \dots, i_n)$.

To any nonlocal game f , let us associate a polynomial $P_f: \mathbb{C}^n \rightarrow \mathbb{C}$ like so: for any n -tuple $(\lambda_1, \dots, \lambda_n)$ of complex numbers, let $P_f(\lambda_1, \dots, \lambda_n)$ be equal to

$$\sum_{(i_1, \dots, i_n) \in \{0, 1\}^n} f(i_1, \dots, i_n) \lambda_1^{i_1} \lambda_2^{i_2} \cdots \lambda_n^{i_n}. \quad (1)$$

For example, if g is the Clauser-Horne-Shimony-Holt (CHSH) game ($g(1, 1) = -1$, $g(0, 0) = g(0, 1) = g(1, 0) = 1$) then

$$P_g = 1 + \lambda_1 + \lambda_2 - \lambda_1 \lambda_2. \quad (2)$$

Additionally, for any binary nonlocal XOR game $f: \{0,1\}^n \rightarrow \mathbb{R}$, and any real numbers $\theta_0, \theta_1, \dots, \theta_n$, let $Z_f(\theta_0, \dots, \theta_n)$ denote the quantity

$$\sum_{(i_k) \in \{0,1\}^n} f(i_1, \dots, i_n) \cos \left(\theta_0 + \sum_k i_k \theta_k \right). \quad (3)$$

Thus, for example, if g is the CHSH game, then

$$Z_g(\theta_0, \theta_1, \theta_2) = \cos(\theta_0) + \cos(\theta_0 + \theta_1) \quad (4)$$

$$+ \cos(\theta_0 + \theta_2) - \cos(\theta_0 + \theta_1 + \theta_2). \quad (5)$$

Note that the function Z_f is 2π -periodic in every variable.

The two quantities P_f and Z_f are related by the following identity.

$$Z_f(\theta_0, \dots, \theta_n) = \text{Re}[e^{i\theta_0} P_f(e^{i\theta_1}, \dots, e^{i\theta_n})]. \quad (6)$$

Note also that

$$|P_f(e^{i\theta_1}, \dots, e^{i\theta_n})| = \max_{t \in [-\pi, \pi]} Z_f(t, \theta_1, \dots, \theta_n). \quad (7)$$

Quantum strategies. For our purposes, a *quantum strategy* for a binary n -player nonlocal game is a pure state

$$|\psi\rangle \in \mathcal{Q}_1 \otimes \mathcal{Q}_2 \otimes \dots \otimes \mathcal{Q}_n, \quad (8)$$

where each \mathcal{Q}_i is a Hilbert space, together with two projective measurements

$$\{P_j^{(0,+)}, P_j^{(0,-)}\}, \{P_j^{(1,+)}, P_j^{(1,-)}\} \quad (9)$$

on the space \mathcal{Q}_j . These measurements can be more compactly expressed as Hermitian operators:

$$M_j^{(0)} := P_j^{(0,+)} - P_j^{(0,-)} \quad (10)$$

$$M_j^{(1)} := P_j^{(1,+)} - P_j^{(1,-)} \quad (11)$$

The *score* for such a strategy is

$$\langle \psi | \sum_{(i_k)} f(i_1, \dots, i_n) M_1^{(i_1)} \otimes \dots \otimes M_n^{(i_n)} | \psi \rangle. \quad (12)$$

Let us use the term *nondegenerate n -qubit strategy* to refer to a strategy whose Hilbert spaces \mathcal{Q}_j are all copies of \mathbb{C}^2 and whose projection operators $P_j^{(i,*)}$ are all one-dimensional projectors.

Proposition 1. *Let $f: \{0,1\}^n \rightarrow \mathbb{R}$ be a nonlocal binary XOR game. Let Q_f denote the optimal score for f that can be achieved by a nondegenerate n -qubit strategy. Then,*

$$Q_f = \max_{|\lambda_1|=\dots=|\lambda_n|=1} |P_f(\lambda_1, \dots, \lambda_n)| \quad (13)$$

and

$$Q_f = \max_{\theta_0, \dots, \theta_n \in [-\pi, \pi]} Z_f(\theta_0, \dots, \theta_n). \quad (14)$$

Proof. Let $\left(\psi, \left\{ \{M_j^{(0)}, M_j^{(1)}\}\}_j \right\} \right)$ be a nondegenerate n -qubit strategy for f . Each of the operators $M_j^{(i)}$ is a Hermitian operator on a 2-dimensional space that has eigenvalues in the set $\{-1, +1\}$. After an appropriate change of basis, we may make the assumption that

$$M_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad M_j^{(1)} = \begin{bmatrix} 0 & e^{i\theta_j} \\ e^{-i\theta_j} & 0 \end{bmatrix} \quad (15)$$

for some $\theta_0, \dots, \theta_n \in [-\pi, \pi]$.

The score for this quantum strategy is clearly bounded by the operator norm of the operator

$$\mathbf{M} := \sum_{(i_k)} f(i_1, \dots, i_n) M_1^{(i_1)} \otimes \dots \otimes M_n^{(i_n)} \quad (16)$$

The operator \mathbf{M} is on a Hilbert space which has basis $\{|a_1 a_2 \dots a_n\rangle \mid a_i \in \{0,1\}\}$. If we take the elements of this basis in lexicographical order, the resulting matrix expression is a reverse-diagonal matrix:

$$\begin{bmatrix} 0 & 0 & \dots & 0 & * \\ 0 & 0 & \dots & * & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & * & \dots & 0 & 0 \\ * & 0 & \dots & 0 & 0 \end{bmatrix} \quad (17)$$

The entries along the reverse diagonal are given by the expressions

$$P_f \left(e^{i(-1)^{a_1} \theta_1}, \dots, e^{i(-1)^{a_n} \theta_n} \right) \quad (18)$$

for $(a_k) \in \{0,1\}^n$.

Using the simple observation that the eigenvalues of any matrix of the form

$$\begin{bmatrix} & & & & z_1 \\ & & & z_2 & \\ & & \dots & & \\ & & z_n & & \\ & \overline{z_n} & & & \\ \dots & & & & \\ \overline{z_2} & & & & \\ \overline{z_1} & & & & \end{bmatrix}, \quad (19)$$

are $\pm |z_1|, \pm |z_2|, \dots, \pm |z_n|$, we find that the operator norm of \mathbf{M} is

$$\max_{(a_i) \in \{0,1\}^n} \left| P_f \left(e^{i(-1)^{a_1} \theta_1}, \dots, e^{i(-1)^{a_n} \theta_n} \right) \right|. \quad (20)$$

Formula (13) follows. Formula (14) follows also via equality (6). \square

Approximation. Let us say that two quantum strategies $(\psi, \{\{M_j^{(0)}, M_j^{(1)}\}\}_j)$ and $(\phi, \{\{N_j^{(0)}, N_j^{(1)}\}\}_j)$ which operate on the same Hilbert spaces $\mathcal{Q}_1, \dots, \mathcal{Q}_n$ are δ -close if

$$\|M_j^{(i)} - N_j^{(i)}\| \leq \delta \quad \forall j \in \{1, 2, \dots, n\}, i \in \{0, 1\},$$

and

$$|\langle \psi, \phi \rangle| \geq 1 - \delta.$$

Let us say that a nonlocal game f satisfies a *second-degree approximation property* if the following holds.

- There exist constants C, ϵ_0 such that any nondegenerate n -qubit strategy whose score is within $\epsilon < \epsilon_0$ of the optimal score is $(C\sqrt{\epsilon})$ -close to an optimal nondegenerate n -qubit strategy.

The next proposition uses the concept of a Hessian matrix. For any twice-differentiable function $G: \mathbb{R}^n \rightarrow \mathbb{R}$ and any element $\mathbf{c} = (c_1, \dots, c_n) \in \mathbb{R}^n$, let

$$\text{Hess}_{\mathbf{c}}(G) = \left[\frac{\partial^2 G}{\partial x_i \partial x_j}(\mathbf{c}) \right]_{i,j}. \quad (21)$$

Proposition 2. *Let $f: \{0, 1\}^n \rightarrow \mathbb{R}$ be a nonlocal binary XOR game. Suppose that the following condition holds: for any global maximum $(\alpha_0, \alpha_1, \dots, \alpha_n)$ of the function $Z_f(\theta_0, \theta_1, \dots, \theta_n)$, the Hessian matrix*

$$\text{Hess}_{(\alpha_0, \dots, \alpha_n)} Z_f \quad (22)$$

is nonsingular. Then, f satisfies a second-degree approximation property.

Proof. Note that the Hessian condition implies that every maximum of the function is an isolated maximum, and therefore there are only a finite number of global maxima (α_k) in the set $[-\pi, \pi]^{n+1}$.

Let s be the maximum value of Z_f (which is the optimal n -qubit score for the nonlocal game f). Additionally, for later use in the proof, let us define another constant. Consider the set

$$\{|P_f(e^{ib_1\alpha_1}, \dots, e^{ib_n\alpha_n})|\}$$

where we let $(\alpha_0, \alpha_1, \dots, \alpha_n)$ vary over all the global maxima for f in the set $[-\pi, \pi]^{n+1}$, and we let (b_k) vary over all sequences in the set $\{-1, 1\}^n$. The largest value in this set is s . Let s_2 denote the second-largest value in this set. (If no such value exists, let $s_2 = 0$.)

Suppose that

$$\left(\psi, \left\{ \left\{ N_j^{(0)}, N_j^{(1)} \right\} \right\}_j \right) \quad (23)$$

is a quantum strategy which achieves score $s - \epsilon$. After a unitary change of basis, we may assume that

$$N_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad N_j^{(1)} = \begin{bmatrix} 0 & e^{i\beta_j} \\ e^{-i\beta_j} & 0 \end{bmatrix}. \quad (24)$$

for some (β_j) .

Let

$$\mathbf{N} = \sum_{(i_k) \in \{0, 1\}^n} f(i_1, \dots, i_n) N_1^{(i_1)} \otimes \dots \otimes N_n^{(i_n)}. \quad (25)$$

We have $\langle \psi | \mathbf{N} | \psi \rangle = s - \epsilon$, and therefore $\|\mathbf{N}\| \geq s - \epsilon$. Writing the operator norm of \mathbf{N} in terms of the function Z_f , we have

$$\max_{\substack{(b_k) \in \{-1, 1\}^n \\ \gamma \in [-\pi, \pi]}} Z_f(\gamma, b_1\beta_1, \dots, b_n\beta_n) \geq s - \epsilon.$$

Thus

$$Z_f(\gamma, d_1\beta_1, \dots, d_n\beta_n) \geq s - \epsilon. \quad (26)$$

for some sequence $(d_k) \in \{-1, 1\}^n$ and some $\gamma \in [-\pi, \pi]$. By Lemma 1.3 from the Supplementary Information, there is a constant C (depending only on f) and a global maximum $(\alpha_0, \alpha_1, \dots, \alpha_n)$ for Z_f such that

$$|d_k\beta_k - \alpha_k| \leq C\sqrt{\epsilon} \quad \forall k \in \{1, 2, \dots, n\}. \quad (27)$$

Let

$$M_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad M_j^{(1)} = \begin{bmatrix} 0 & e^{id_j\alpha_j} \\ e^{-id_j\alpha_j} & 0 \end{bmatrix}.$$

Note that

$$\|M_j^{(i)} - N_j^{(i)}\| \leq C\sqrt{\epsilon}. \quad (28)$$

Let

$$\mathbf{M} = \sum_{(i_k) \in \{0, 1\}^n} f(i_1, \dots, i_n) M_1^{(i_1)} \otimes \dots \otimes M_n^{(i_n)}.$$

The eigenvalues of this operator are given by

$$\{|P_f(e^{ib_1\alpha_1}, \dots, e^{ib_n\alpha_n})| \mid (b_k) \in \{-1, 1\}^n\},$$

and its largest eigenvalue is s .

Consider the quantity $\|\mathbf{M} - \mathbf{N}\|$. Let p be the sum of the absolute values of the coefficients of $P_f(\lambda_0, \dots, \lambda_n)$. An easy triangle-inequality argument based on (27) shows that the absolute value of any entry of $\mathbf{M} - \mathbf{N}$ is bounded by $npC\sqrt{\epsilon}$. Therefore,

$$\|\mathbf{M} - \mathbf{N}\| \leq npC\sqrt{\epsilon}. \quad (29)$$

Thus,

$$\langle \psi | \mathbf{M} | \psi \rangle \geq \langle \psi | \mathbf{N} | \psi \rangle - \|\mathbf{M} - \mathbf{N}\| \quad (30)$$

$$\geq s - \epsilon - npC\sqrt{\epsilon}. \quad (31)$$

The quantity s_2 defined earlier is an upper bound for all the eigenvalues of \mathbf{M} except for s . By Lemma 2.1 from the Supplementary Information, there exists an s -eigenvector ϕ for \mathbf{M} such that

$$|\langle \psi | \phi \rangle|^2 \geq 1 - \left(\frac{\epsilon + npC\sqrt{\epsilon}}{s - s_2} \right), \quad (32)$$

and therefore

$$|\langle \psi | \phi \rangle| \geq 1 - \left(\frac{\epsilon + npC\sqrt{\epsilon}}{s - s_2} \right). \quad (33)$$

All constants in the expression in parantheses above are independent of the chosen strategy (23), and this expression is $O(\sqrt{\epsilon})$ as $\epsilon \rightarrow 0$. The above inequality combined with (28) gives the desired result. \square

Self-testing. Let f be a binary nonlocal XOR game, and let $\phi \in (\mathbb{C}^2)^{\otimes n}$ be an n -qubit state. Let us say that f is a *self-test* for ϕ if the following condition holds:

- For any optimal nondegenerate n -qubit strategy $(\psi, \{\{M_j^{(0)}, M_j^{(1)}\}\}_j)$, there exist unitary matrices $U_j: \mathbb{C}^2 \rightarrow \mathbb{C}^2$ such that

$$\psi = (U_1 \otimes U_2 \otimes \dots \otimes U_n)\phi. \quad (34)$$

Proposition 3. *Let $f: \{0,1\}^n \rightarrow \mathbb{R}$ be a nonlocal binary XOR game. Suppose that the function Z_f has exactly two maxima in the set $[-\pi, \pi]^{n+1}$, and that these two maxima are of the form $(\alpha_0, \alpha_1, \dots, \alpha_n)$ and $(-\alpha_0, -\alpha_1, \dots, -\alpha_n)$, with $\alpha_i \notin \{-\pi, 0, \pi\}$ for all $i \in \{1, 2, \dots, n\}$. Then, f is a self-test for some n -qubit state ϕ .*

Proof. Let

$$\phi = \frac{1}{\sqrt{2}} \left(|00 \dots 0\rangle + \frac{P_f(\alpha_1, \dots, \alpha_n)}{|P_f(\alpha_1, \dots, \alpha_n)|} |11 \dots 1\rangle \right).$$

Suppose that $(\psi, \{\{M_j^{(0)}, M_j^{(1)}\}\}_j)$ is an optimal nondegenerate n -qubit strategy for f . After a unitary change of basis, we may assume that the operators $M_j^{(i)}$ have the form

$$M_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad M_j^{(1)} = \begin{bmatrix} 0 & e^{i\theta_j} \\ e^{-i\theta_j} & 0 \end{bmatrix}, \quad (35)$$

with $(\theta_j) \in [-\pi, \pi]^n$, and we may make the additional assumption that the vectors $(\alpha_1, \dots, \alpha_n)$ and $(\theta_1, \dots, \theta_n)$ lie in the same quadrant. (That is, $\alpha_j > 0 \iff \theta_j > 0$ for all j .)

Again we let

$$\mathbf{M} = \sum_{(i_k)} f(i_1, \dots, i_n) M_1^{(i_1)} \otimes \dots \otimes M_n^{(i_n)}. \quad (36)$$

Since the chosen strategy is optimal, by formula (20) we must have $(\theta_1, \dots, \theta_n) = (\alpha_1, \dots, \alpha_n)$. Moreover, the vector ψ must lie in the eigenspace corresponding to the largest eigenvalue of \mathbf{M} . This eigenspace is spanned by ϕ . The result follows. \square

Example. Let us illustrate the previous propositions with the example of the Greenberger-Horne-Zeilinger (GHZ) paradox. Define a function $h: \{0,1\}^3 \rightarrow \mathbb{R}$ by

$$\begin{aligned} h(0,0,0) &= 1 \\ h(0,1,1) &= h(1,0,1) = h(1,1,0) = -1 \\ h(0,0,1) &= h(0,1,0) = h(1,0,0) = h(1,1,1) = 0. \end{aligned}$$

Then,

$$\begin{aligned} Z_h(\theta_0, \theta_1, \theta_2, \theta_3) &= \cos(\theta_0) - \cos(\theta_0 + \theta_1 + \theta_2) \\ &\quad - \cos(\theta_0 + \theta_1 + \theta_3) - \cos(\theta_0 + \theta_2 + \theta_3). \end{aligned}$$

It is easily seen that Z_h has two maxima inside the region $[-\pi, \pi]^4$: $(0, \frac{\pi}{2}, \frac{\pi}{2}, \frac{\pi}{2})$ and $(0, -\frac{\pi}{2}, -\frac{\pi}{2}, -\frac{\pi}{2})$. Therefore by Proposition 3, h is a self-test for a 3-qubit state. (In fact, it is a self-test for the GHZ state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.) Moreover, the Hessian at both of these maxima is equal to

$$\begin{bmatrix} -4 & -2 & -2 & -2 \\ -2 & -2 & -1 & -1 \\ -2 & -1 & -2 & -1 \\ -2 & -1 & -1 & -2 \end{bmatrix}, \quad (37)$$

which is nonsingular.

Combining Propositions 2 and 3, we have the following: for any state $\psi \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ which is part of a nondegenerate strategy that achieves score $1 - \epsilon$, there is a state ψ' which is equivalent to ψ under local unitary transformation satisfying

$$|\langle \psi', GHZ \rangle| \geq 1 - C\sqrt{\epsilon} \quad (38)$$

where C is a fixed constant.

The reader can compare this to the non-robust self-testing result of Colbeck ([8], Appendix C).

General quantum strategies. Now suppose that we consider quantum strategies of arbitrary dimension. Whenever there are two projective binary measurements $\{P^{(0,+)}, P^{(1,-)}\}, \{P^{(1,+)}, P^{(0,-)}\}$ on a single Hilbert space \mathcal{Q} , there exists a decomposition

$$\mathcal{Q} = \bigoplus_{\ell=1}^m \mathcal{Q}_\ell \quad (39)$$

which is respected by each of the projections $P^{(i,*)}$, with $\dim \mathcal{Q}_\ell \leq 2$.¹ This allows us to reduce general quantum strategies to n -qubit strategies. Using this fact, the following generalizations of Propositions 1, 2, and 3 can be proved.

Proposition 4. *Let f be a binary nonlocal XOR game. Let Q'_f be the supremum of the scores achieved by quantum strategies (of any dimension) for the game f . Then, Q'_f is equal to the quantity Q_f from Proposition 1.* \square

¹ See Lemma 1 from O. Regev's lecture notes, www.cs.tau.ac.il/~odedr/teaching/quantum_fall_2005/ln/qma.pdf.

Proposition 5. *Let f be a binary nonlocal XOR game which satisfies the condition of Proposition 2. Then, there exists a constant $C > 0$ such that the following holds. For any quantum strategy*

$$\psi \in \mathcal{Q}_1 \otimes \dots \otimes \mathcal{Q}_n, \quad (40)$$

$$\left\{ M_j^{(i)} : \mathcal{Q}_j \rightarrow \mathcal{Q}_j \right\}_{i,j} \quad (41)$$

whose score is within ϵ of the optimal score s , there exists a quantum strategy

$$\phi \in \mathcal{R}_1 \otimes \dots \otimes \mathcal{R}_n, \quad (42)$$

$$\left\{ N_j^{(i)} : \mathcal{R}_j \rightarrow \mathcal{R}_j \right\}_{i,j} \quad (43)$$

achieving score s and unitary embeddings

$$U_j : \mathcal{Q}_j \hookrightarrow \mathcal{R}_j \quad (44)$$

such that

$$|\langle (U_1 \otimes \dots \otimes U_n) \psi, \phi \rangle| \geq 1 - C\sqrt{\epsilon}. \quad \square \quad (45)$$

Proposition 6. *Let f be a binary nonlocal XOR game which satisfies the conditions of Proposition 3. Then, there exists an n -qubit state $\alpha \in (\mathbb{C}^2)^{\otimes n}$ such that the following holds: for any n -partite state $\psi \in \mathcal{Q}_1 \otimes \dots \otimes \mathcal{Q}_n$ which is part of an optimal strategy for f , there exists another n -partite state $\lambda \in \mathcal{Q}'_1 \otimes \dots \otimes \mathcal{Q}'_n$ and unitary embeddings $V_j : \mathcal{Q}_j \hookrightarrow \mathbb{C}^2 \otimes \mathcal{Q}'_j$ such that*

$$(V_1 \otimes \dots \otimes V_n) |\psi\rangle = |\alpha\rangle \otimes |\lambda\rangle. \quad \square \quad (46)$$

Conclusion. We have provided a general scheme for proving robust self-testing results in the context of binary XOR games, and we have applied it to prove a new result

on the GHZ paradox. A natural question is whether the scheme can be generalized beyond binary games. Such generalization may be difficult since some of the mathematical tools we have used (such as the canonical form (15) and the decomposition (39)) break down when non-binary inputs and outputs are allowed. Some new mathematical insight may be required to extend our results.

It would be interesting to try to apply the GHZ result to randomness expansion, following proposals such as those in [3] and [9].

* carlmi@umich.edu

† shiyy@umich.edu

- [1] S. Popescu and D. Rohrlich, *Physical Letters A* **169**, 411 (1992).
- [2] D. Mayers and A. Yao, *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* pp. 503–509 (1998).
- [3] R. Colbeck and A. Kent, *J. Phys. A: Math. Theor.* **44**, 095305 (2011).
- [4] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al., *Nature* **464**, 1021 (2010).
- [5] M. McKague, T. Z. Yang, and V. Scarani, *arXiv:1204.2976v1* (2012).
- [6] C. Miller and Y. Shi, *Randomness expansion from the Greenberger-Horne-Zeilinger paradox* (2011), attached to this manuscript.
- [7] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, *Physical Review Letters* **108**, 260502 (2012).
- [8] R. Colbeck, *Quantum and relativistic protocols for secure multi-party computation* (2006), Ph. D. thesis, University of Cambridge.
- [9] R. Colbeck and R. Renner, *Nature Physics* **8**, 450 (2012).

SUPPLEMENTARY INFORMATION

1. LEMMAS FOR MULTIVARIABLE FUNCTIONS

For any twice-differentiable function $F: \mathbb{R}^n \rightarrow \mathbb{R}$ and any $\mathbf{c} = (c_1, \dots, c_n) \in \mathbb{R}^n$, let $\text{Hess}_{\mathbf{c}}F$ denote the Hessian matrix,

$$\text{Hess}_{\mathbf{c}}F := \begin{bmatrix} \frac{\partial^2}{\partial z_1^2} F & \frac{\partial}{\partial z_1} \frac{\partial}{\partial z_2} F & \dots & \frac{\partial}{\partial z_1} \frac{\partial}{\partial z_n} F \\ \frac{\partial}{\partial z_2} \frac{\partial}{\partial z_1} F & \frac{\partial^2}{\partial z_2^2} F & \dots & \frac{\partial}{\partial z_2} \frac{\partial}{\partial z_n} F \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial}{\partial z_n} \frac{\partial}{\partial z_1} F & \frac{\partial}{\partial z_n} \frac{\partial}{\partial z_2} F & \dots & \frac{\partial^2}{\partial z_n^2} F \end{bmatrix} (c_1, \dots, c_n).$$

Lemma 1.1. *Let $G: \mathbb{R}^n \rightarrow \mathbb{R}$ be a twice-differentiable function. Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ be such that all first order partial derivatives of G vanish at \mathbf{x} , and the Hessian matrix $\text{Hess}_{\mathbf{x}}(G)$ is negative definite. Then, there exist constants $\delta_0, C > 0$ such that for all $\mathbf{y} \in \mathbb{R}^n$ with $\|\mathbf{y} - \mathbf{x}\|^2 < \delta_0$,*

$$(1) \quad G(\mathbf{y}) \leq G(\mathbf{x}) - C \|\mathbf{x} - \mathbf{y}\|^2.$$

Proof. Let λ be the eigenvalue of $\text{Hess}_{\mathbf{x}}(G)$ that is closest to zero, and let $C = -\lambda/2$. Define a function $F: \mathbb{R}^n \rightarrow \mathbb{R}$ by

$$(2) \quad F(\mathbf{y}) = G(\mathbf{y}) + C \|\mathbf{y} - \mathbf{x}\|^2.$$

Then, the Hessian of F at \mathbf{x} is

$$(3) \quad \text{Hess}_{\mathbf{x}}(F) = \text{Hess}_{\mathbf{x}}(G) + C \mathbb{I}_n,$$

which is negative definite. Therefore, \mathbf{x} is a local maximum of F . The result follows. \square

For any vector $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$, let $\|\mathbf{y}\|_{\infty} = \max_i |y_i|$. Note that

$$(4) \quad \|\mathbf{y}\|_{\infty} \leq \|\mathbf{y}\| \leq \sqrt{n} \|\mathbf{y}\|_{\infty}.$$

The following modification of Lemma 1.1 follows immediately.

Lemma 1.2. *Let $G: \mathbb{R}^n \rightarrow \mathbb{R}$ be a twice-differentiable function. Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ be such that all first order partial derivatives of G vanish at \mathbf{x} , and the Hessian matrix $\text{Hess}_{\mathbf{x}}(G)$ is negative definite. Then, there exist constants $\delta_0, C > 0$ such that for all $\mathbf{y} \in \mathbb{R}^n$ with $\|\mathbf{y} - \mathbf{x}\|_{\infty}^2 < \delta_0$,*

$$(5) \quad G(\mathbf{y}) \leq G(\mathbf{x}) - C \|\mathbf{x} - \mathbf{y}\|_{\infty}^2. \quad \square$$

For any set $S \in \mathbb{R}^n$ and any $\delta > 0$, let

$$(6) \quad B_{\infty}^{\delta}(S) = \{\mathbf{y} \in \mathbb{R}^n \mid \exists \mathbf{x} \in S \text{ such that } \|\mathbf{x} - \mathbf{y}\|_{\infty} \leq \delta\}.$$

Lemma 1.3. *Let $G: \mathbb{R}^n \rightarrow \mathbb{R}$ be a twice-differentiable function. Let c be a positive real number. Let b be the maximum value of G achieved on the set $[-c, c]^n$. Suppose that this maximum is achieved only by a finite number of points $\{\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)}\}$, all of which occur in the interior of $[-c, c]^n$. Suppose also that*

$$(7) \quad \det \text{Hess}_{\mathbf{x}^{(i)}}(G) \neq 0$$

for all $i \in \{1, \dots, m\}$. Then, there exists a constant $K > 0$ such that for all $\epsilon > 0$,

$$(8) \quad G^{-1}([b - \epsilon, b]) \subseteq B_{\infty}^{K\sqrt{\epsilon}}(Y).$$

Proof. By Lemma 1.2, there exist constants $C, \epsilon_0 > 0$ such that for any $i \in \{1, \dots, m\}$ and any $\mathbf{y} \in \mathbb{R}^n$ such that $\|\mathbf{y} - \mathbf{x}^{(i)}\|_{\infty} \leq \epsilon_0$,

$$(9) \quad G(\mathbf{y}) \leq G(\mathbf{x}^{(i)}) - C \|\mathbf{x}^{(i)} - \mathbf{y}\|_{\infty}^2.$$

Let b' be the largest value achieved by G on the compact set

$$(10) \quad \left\{ \mathbf{y} \in [-c, c]^n \mid \|\mathbf{y} - \mathbf{x}^{(i)}\|_{\infty} \geq \epsilon_0 \quad \forall i \in \{1, \dots, m\} \right\}.$$

Setting

$$(11) \quad K = \max \left\{ C^{-1}, \frac{2c}{\sqrt{b - b'}} \right\}$$

yields the result. \square

2. A LEMMA FOR HERMITIAN OPERATORS

Lemma 2.1. *Let X is an $n \times n$ Hermitian operator. Suppose that r is the largest eigenvalue of X , and suppose that r' is a quantity that is less than r but greater than or equal to all other eigenvalues of X . Suppose that v is a unit vector such that*

$$(12) \quad \langle v | X | v \rangle \geq r - \epsilon.$$

Then, there exists a unit r -eigenvector u for X such that

$$(13) \quad |\langle u | v \rangle|^2 \geq 1 - \frac{\epsilon}{r - r'}.$$

Proof. Let V denote the r -eigenspace for X , and let V^{\perp} denote its complement. Let

$$(14) \quad X' = r \cdot \text{proj}_V + r' \cdot \text{proj}_{V^{\perp}}.$$

Then, $X' \geq X$, and thus

$$(15) \quad \langle v | X' | v \rangle \geq \langle v | X | v \rangle \geq r - \epsilon.$$

Since

$$(16) \quad \langle v | X' | v \rangle = r \|\text{proj}_V v\|^2 + r' \|\text{proj}_{V^{\perp}} v\|^2$$

$$(17) \quad = r \|\text{proj}_V v\|^2 + r' (1 - \|\text{proj}_V v\|^2)$$

we therefore have

$$(18) \quad r \|\text{proj}_V v\|^2 + r' (1 - \|\text{proj}_V v\|^2) \geq r - \epsilon.$$

By an algebraic manipulation,

$$(19) \quad \|\text{proj}_V v\|^2 \geq 1 - \frac{\epsilon}{r - r'}.$$

Letting $u = \mathbf{proj}_V v / \|\mathbf{proj}_V v\|$ yields the result.

□

Randomness Expansion from the Greenberger-Horne-Zeilinger Paradox*

Carl A. Miller Yaoyun Shi

A Randomness Expansion Devices

In this section, we formalize the notion of a multi-part *randomness expansion* (RE) device.

A **3-part randomness expansion (RE) device** D is a device consisting of 3 components, D_1 , D_2 , D_3 , satisfying all of the following conditions:

1. Each component D_j accepts a single bit $i_j \in \{0, 1\}$ as input and returns a single bit $o_j \in \{0, 1\}$ as output.
2. Each component D_j contains a quantum system, Q_j . When it receives its input bit i_j , it performs an orthogonal binary measurement on Q_j . The output bit o_j is the result of this measurement.
3. The choice of measurement performed by D_j is determined solely by its input bit i_j . In particular, it does not depend on the inputs or outputs of any of the other components. (The components do not communicate with one another.)

We will say that the input bits (i_j) and the output bits (o_j) **pass the GHZ test** if the following Boolean relations are satisfied:

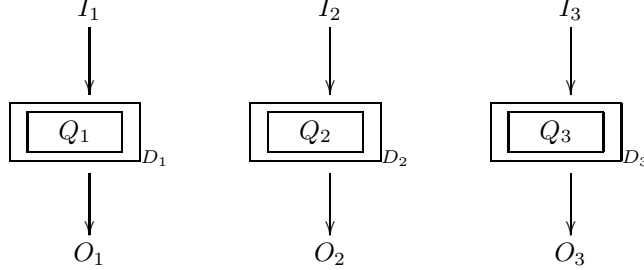
$$i_1 \oplus i_2 \oplus i_3 = 0, \tag{1}$$

$$o_1 \oplus o_2 \oplus o_3 \oplus (i_1 \vee i_2 \vee i_3) = 1. \tag{2}$$

In what follows, we will often be choosing the inputs to device D according to a random probability distribution. In this case, we denote the inputs by the random variables I_1 , I_2 , and I_3 , and the outputs by the random variables O_1 ,

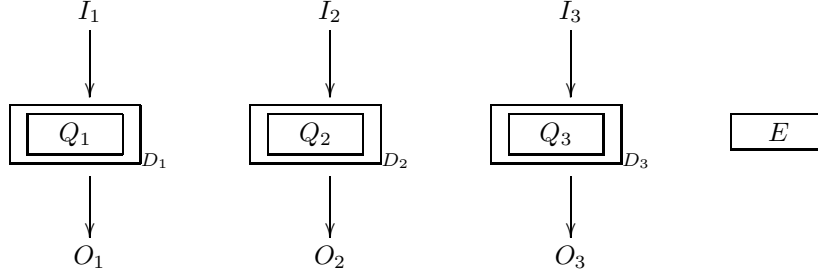
*This appendix was written during June - August 2011. The text given here is unmodified except for a few minor edits.

O_2 , and O_3 . Let $I = (I_1, I_2, I_3)$, and $O = (O_1, O_2, O_3)$.



Let Q denote the tripartite quantum system formed by Q_1 , Q_2 , and Q_3 . As a convention, if Z is a quantum system, then we use the corresponding symbol \mathcal{Z} to denote the complex Euclidean state-space of Z . Thus \mathcal{Q}_1 , \mathcal{Q}_2 , and \mathcal{Q}_3 denote the state spaces of Q_1 , Q_2 , and Q_3 .

Note that the state of the system Q may be mixed. Sometimes we will consider an additional quantum system that is entangled with Q :



We will use the expressions $\Gamma_*^{(pre)}$ and $\Gamma_*^{(post)}$ to denote the pre- and post-measurements states of the systems above. Thus,

$$\Gamma_{IQE}^{(post)} \quad (3)$$

denotes the post-measurement state of the systems I , Q , and E , taken together. We will drop the “(pre)” and “(post)” superscripts when they are not necessary.

Γ is always presumed to denote a density operator. If the state of a collection of quantum systems happens to be pure, then we may also use the symbol v to denote the vector representing the pure state. (Thus for example, if the expression $v_Q^{(pre)}$ appears, it should be interpreted to mean a vector in \mathcal{Q} representing the pure pre-measurement state of \mathcal{Q} .)

A.1 A canonical form

Let D be a 3-part RE device (as defined above). For any $j \in \{1, 2, 3\}$, and any input bit $i \in \{0, 1\}$, let

$$\{P_j^{(i,o)}\}_{o \in \{0,1\}} \quad (4)$$

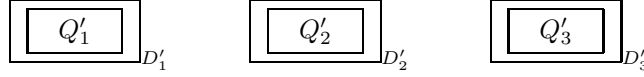
be the orthogonal measurement the the component D_j performs on its quantum system Q_j on input i . This is a set consisting of two complementary orthogonal projection operators on the space \mathcal{Q}_j .

It is convenient to express (4) as a single operator. Let

$$T_j^{(i)} = P_j^{(i,0)} - P_j^{(i,1)}. \quad (5)$$

This is a Hermitian operator on \mathcal{Q}_j whose square is equal to \mathbb{I} . In general, any Hermitian operator X satisfying $X^2 = \mathbb{I}$ yields a binary orthogonal measurement $(\{\frac{\mathbb{I}+X}{2}, \frac{\mathbb{I}-X}{2}\})$. For this reason, we will often refer to such an operator X simply as a “measurement.”

Let D' be another 3-part RE device,



whose measurements are denoted by $T_j'^{(i)}$. Let us say that a **unitary embedding** of D into D' is a collection of unitary embeddings

$$\begin{aligned} \Psi_1 &: \mathcal{Q}_1 \hookrightarrow \mathcal{Q}'_1 \\ \Psi_2 &: \mathcal{Q}_2 \hookrightarrow \mathcal{Q}'_2 \\ \Psi_3 &: \mathcal{Q}_3 \hookrightarrow \mathcal{Q}'_3 \end{aligned}$$

which map the pre-measurement state of $Q = (Q_1, Q_2, Q_3)$ to the pre-measurement state of $Q' = (Q'_1, Q'_2, Q'_3)$, and which are such that

$$T_j^{(i)} = \Psi_j^\dagger \left(T_j'^{(i)} \right) \Psi_j \quad (6)$$

It is easy to see that if such a unitary embedding exists, then the device D' has the same output-statistics as D .

If E is an additional quantum system, and the pre-measurement states of D and D' are given as entangled states

$$\Gamma_{QE}^{(pre)} \text{ and } \Gamma_{Q'E}^{(pre)},$$

then we say that the unitary embedding (Ψ_i) **respects entanglement with E** if the superoperator

$$(\Psi_1 \otimes \Psi_2 \otimes \Psi_3 \otimes \mathbb{I}_E) (\cdot) (\Psi_1 \otimes \Psi_2 \otimes \Psi_3 \otimes \mathbb{I}_E)^\dagger \quad (7)$$

carries $\Gamma_{QE}^{(pre)}$ to $\Gamma_{Q'E}^{(pre)}$.

Proposition A.1. *Let D be a 3-part RE device which is entangled with an additional quantum system E . Then there exists a unitary embedding of D into another 3-part RE device D' , respecting entanglement with E , such that the following conditions hold.*

1. The state-spaces of D' have the form

$$\mathcal{Q}'_1 = \mathcal{A} \otimes \mathcal{R}_1 \quad (8)$$

$$\mathcal{Q}'_2 = \mathcal{B} \otimes \mathcal{R}_2 \quad (9)$$

$$\mathcal{Q}'_3 = \mathcal{C} \otimes \mathcal{R}_3. \quad (10)$$

where \mathcal{A} , \mathcal{B} , and \mathcal{C} are complex Euclidean spaces, and \mathcal{R}_1 , \mathcal{R}_2 , and \mathcal{R}_3 are copies of $\mathbb{C}^{\{0,1\}}$.

2. The measurements operators for D'_j on input $i = 0$ are given, respectively, by

$$\sum_k |a_k\rangle \langle a_k| \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (11)$$

$$\sum_\ell |b_\ell\rangle \langle b_\ell| \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (12)$$

$$\sum_m |c_m\rangle \langle c_m| \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (13)$$

where $\{a_k\}$, $\{b_\ell\}$, and $\{c_m\}$ denote orthogonal bases for \mathcal{A} , \mathcal{B} , and \mathcal{C} .¹

3. The measurements operators for D'_j on input $i = 1$ are given by

$$\sum_k |a_k\rangle \langle a_k| \otimes \begin{bmatrix} 0 & \lambda_k \\ \lambda_k & 0 \end{bmatrix}, \quad (14)$$

$$\sum_\ell |b_\ell\rangle \langle b_\ell| \otimes \begin{bmatrix} 0 & \gamma_\ell \\ \gamma_\ell & 0 \end{bmatrix}, \quad (15)$$

$$\sum_m |c_m\rangle \langle c_m| \otimes \begin{bmatrix} 0 & \phi_m \\ \phi_m & 0 \end{bmatrix}, \quad (16)$$

where λ_k , γ_ℓ , and ϕ_m denote complex numbers that satisfy

$$|\lambda_k| = |\gamma_\ell| = |\phi_m| = 1, \quad (17)$$

$$\text{Im}(\lambda_k) \geq 0, \quad (18)$$

$$\text{Im}(\gamma_\ell) \geq 0, \quad (19)$$

$$\text{Im}(\phi_m) \geq 0. \quad (20)$$

Proof. It is easy to show that, given any two Hermitian operators X and Y on \mathbb{C}^2 such that $X^2 = Y^2 = \mathbb{I}$, there is a unitary transformation $U: \mathbb{C}^2 \rightarrow \mathbb{C}^2$ such that

$$UXU^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (21)$$

$$UYU^\dagger = \begin{bmatrix} 0 & \zeta \\ \bar{\zeta} & 0 \end{bmatrix}, \quad (22)$$

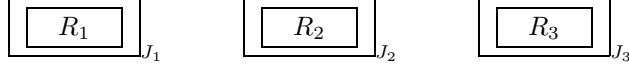
¹The 2×2 matrices here are written with respect to the computational basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{C}^{\{0,1\}}$.

where ζ satisfies $|\zeta| = 1$ and $\text{Im}(\zeta) \geq 0$. From this fact, it is easy to prove the proposition for the case where the spaces \mathcal{Q}_j all have dimension ≤ 2 . The general case then follows via Jordan's lemma.² \square

B The GHZ Paradox: $2 \times 2 \times 2$ case

We are interested in those RE devices which pass the GHZ test (see (2)) with high probability. Because of Proposition A.1, it is useful to focus on RE devices that are in a particular form.

Let J be a 3-part RE device.



Suppose that $\mathcal{R}_j = \mathbb{C}^{\{0,1\}}$ for each j , and suppose that the measurement operators $\{S_j^{(i)}\}$ for J are given by

$$S_1^{(0)} = S_2^{(0)} = S_3^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (23)$$

$$S_1^{(1)} = \begin{bmatrix} 0 & \lambda \\ \bar{\lambda} & 0 \end{bmatrix} \quad (24)$$

$$S_2^{(1)} = \begin{bmatrix} 0 & \gamma \\ \bar{\gamma} & 0 \end{bmatrix} \quad (25)$$

$$S_3^{(1)} = \begin{bmatrix} 0 & \phi \\ \bar{\phi} & 0 \end{bmatrix} \quad (26)$$

with $|\lambda| = |\gamma| = |\phi| = 1$. Suppose that the pre-measurement state of (R_1, R_2, R_3) is a pure state given by a vector $\alpha \in \mathcal{R}_1 \otimes \mathcal{R}_2 \otimes \mathcal{R}_3$.

Consider that a 3-bit string $I_1 I_2 I_3$ is chosen uniformly at random from the set

$$\{000, 011, 101, 110\}, \quad (27)$$

and given to device J . Then J passes the GHZ test if and only if the output string $O_1 O_2 O_3$ satisfies the relation

$$O_1 \oplus O_2 \oplus O_3 \oplus (I_1 \vee I_2 \vee I_3) = 1. \quad (28)$$

We can calculate the probability that this formula will be satisfied using the operators $S_j^{(i)}$. For example, the probability that the formula will be satisfied when the input string is 110 is:

$$\frac{1}{2} + \frac{1}{2} \left\langle \left(S_1^{(1)} \otimes S_2^{(1)} \otimes S_3^{(0)} \right) \alpha, \alpha \right\rangle \quad (29)$$

²See Lemma 1 from http://www.cs.tau.ac.il/~odedr/teaching/quantum_fall_2005/ln/qma.pdf.

The probability that this formula will be satisfied on an input randomly chosen from (27) is

$$\begin{aligned} \frac{1}{2} & - \frac{1}{8} \left\langle \left(S_1^{(0)} \otimes S_2^{(0)} \otimes S_3^{(0)} \right) \alpha, \alpha \right\rangle \\ & + \frac{1}{8} \left\langle \left(S_1^{(0)} \otimes S_2^{(1)} \otimes S_3^{(1)} \right) \alpha, \alpha \right\rangle \\ & + \frac{1}{8} \left\langle \left(S_1^{(1)} \otimes S_2^{(0)} \otimes S_3^{(1)} \right) \alpha, \alpha \right\rangle \\ & + \frac{1}{8} \left\langle \left(S_1^{(1)} \otimes S_2^{(1)} \otimes S_3^{(0)} \right) \alpha, \alpha \right\rangle \end{aligned} \quad (30)$$

Let

$$\alpha = \sum_{k,l,m \in \{0,1\}} c_{klm} |klm\rangle. \quad (31)$$

Writing (30) in terms of λ , γ , ϕ , and $\{c_{jkl}\}$, and rearranging terms, we find the following expression:

$$\begin{aligned} \mathbf{P}(J \text{ passes the GHZ test}) &= \frac{1}{2} + \operatorname{Re} \left[\overline{c_{111}} \cdot c_{000} \left(\frac{-1 + \lambda\gamma + \gamma\phi + \phi\lambda}{4} \right) \right] \\ &+ \operatorname{Re} \left[\overline{c_{110}} \cdot c_{001} \left(\frac{-1 + \lambda\gamma + \gamma\bar{\phi} + \bar{\phi}\lambda}{4} \right) \right] \\ &+ \operatorname{Re} \left[\overline{c_{101}} \cdot c_{010} \left(\frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\phi + \phi\lambda}{4} \right) \right] \\ &+ \operatorname{Re} \left[\overline{c_{100}} \cdot c_{011} \left(\frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\bar{\phi} + \bar{\phi}\lambda}{4} \right) \right]. \end{aligned}$$

We will make frequent use of this expression in the subsections that follow.

B.1 A Few Lemmas

The following lemmas will be useful in subsequent sections.

Lemma B.1. *Let a , b , and c be complex numbers such that $|a| = |b| = |c| = 1$ and $\operatorname{Im}(a) \geq 0$, $\operatorname{Im}(b) \geq 0$, and $\operatorname{Im}(c) \geq 0$. Then,*

$$\left| \frac{-1 + ab + bc + ca}{4} \right| \leq \sqrt{1 - \frac{|a - i|^2}{4}}. \quad (32)$$

Proof. Consider, for all complex numbers b' satisfying $|b'| = 1$, the value

$$|-1 + ab' + b'c + ca| = |(-1 + ca) + b'(a + c)|. \quad (33)$$

This value will be maximized when the angle of $(-1 + ca)$ in the complex plane agrees with the angle of $b'(a + c)$. This occurs precisely when $b' = i$. Therefore,

$$|-1 + ab + bc + ca| \leq |-1 + ai + ic + ca|. \quad (34)$$

By similar reasoning,

$$|-1 + ai + ic + ca| \leq |-1 + ai + i^2 + ia|. \quad (35)$$

Therefore,

$$|-1 + ab + bc + ca| \leq |-2 + 2ai| = |2a + 2i| \quad (36)$$

Note that $|2a + 2i|^2 + |2a - 2i|^2 = 16$. Therefore,

$$|-1 + ab + bc + ca|^2 \leq |2a + 2i|^2 \quad (37)$$

implies

$$|-1 + ab + bc + ca|^2 \leq 16 - |2a - 2i|^2. \quad (38)$$

Dividing by 16 and taking square roots of both sides of the equation yields the result. \square

Lemma B.2. *Let a , b , and c be complex numbers such that $|a| = |b| = |c| = 1$. Suppose that $\text{Im}(a) \geq 0$ and $\text{Im}(b) \geq 0$, but $\text{Im}(c) \leq 0$. Then,*

$$\left| \frac{-1 + ab + bc + ca}{4} \right| \leq \frac{\sqrt{2}}{2}. \quad (39)$$

Proof. Consider the complex numbers

$$(-1 + ab) \quad \text{and} \quad (a + b). \quad (40)$$

In the complex plane, $(-1 + ab)$ lies at an angle of $+\pi/2$ (in the counterclockwise direction) from $(a + b)$. Since $\text{Im}(c) \leq 0$, the angle between the product $c(a + b)$ and $(-1 + ab)$ must be an obtuse angle or a right angle. Therefore,

$$|(-1 + ab) + c(a + b)|^2 \leq |-1 + ab|^2 + |a + b|^2 \leq 8. \quad (41)$$

The lemma follows. \square

Lemma B.3. *Suppose that A , B , A' and B' are Hermitian operators on \mathbb{C}^n which satisfy $\|\cdot\|_\infty \leq 1$. Then,*

$$\|A \otimes B - A' \otimes B'\|_\infty \leq \|A - A'\|_\infty + \|B - B'\|_\infty. \quad (42)$$

Proof. We have the following:

$$\|A \otimes B - A' \otimes B'\|_\infty = \|(A - A') \otimes B + A' \otimes (B - B')\|_\infty \quad (43)$$

$$\leq \|A - A'\|_\infty \|B\|_\infty + \|A'\|_\infty \|B - B'\|_\infty \quad (44)$$

$$\leq \|A - A'\|_\infty + \|B - B'\|_\infty. \quad (45)$$

\square

B.2 Characterizing Approximate GHZ Devices

There exists 3-part RE devices which satisfy the GHZ test perfectly. Consider the 3-qubit device whose pre-measurement state is the pure state

$$g = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \in \mathbb{C}^{\{0,1\}} \otimes \mathbb{C}^{\{0,1\}} \otimes \mathbb{C}^{\{0,1\}} \quad (46)$$

and which is the such that each component uses the measurement operator

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (47)$$

on input $i = 0$, and the measurement operator

$$\sigma_y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \quad (48)$$

on input $i = 1$. This device passes the GHZ test with probability 1. Let us refer to this device as **the ideal GHZ device**.

We will use the above example for comparison. In the next two propositions, we see that if a $2 \times 2 \times 2$ RE device passes the GHZ test with high probability, then it is similar to an ideal GHZ device.

Proposition B.4. *Let J be a 3-part RE device whose state spaces \mathcal{R}_j are copies of the qubit-space $\mathbb{C}^{\{0,1\}}$, and whose pre-measurement state is a pure state*

$$\alpha = \sum_{k,l,m \in \{0,1\}} c_{klm} |klm\rangle. \quad (49)$$

Suppose that the measurement operators for J are

$$\begin{aligned} S_1^{(0)} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & S_2^{(0)} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & S_3^{(0)} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ S_1^{(1)} &= \begin{bmatrix} 0 & \lambda \\ \bar{\lambda} & 0 \end{bmatrix} & S_2^{(1)} &= \begin{bmatrix} 0 & \gamma \\ \bar{\gamma} & 0 \end{bmatrix} & S_3^{(1)} &= \begin{bmatrix} 0 & \phi \\ \bar{\phi} & 0 \end{bmatrix} \end{aligned} \quad (50)$$

where

$$|\lambda| = |\gamma| = |\phi| = 1 \quad (51)$$

$$\text{Im}(\lambda) \geq 0 \quad (52)$$

$$\text{Im}(\gamma) \geq 0 \quad (53)$$

$$\text{Im}(\phi) \geq 0. \quad (54)$$

Suppose that

$$\mathbf{P}(J \text{ passes the GHZ test}) = 1 - \epsilon. \quad (55)$$

Then,

$$|\lambda - i|^2 \leq 16\epsilon \quad (56)$$

$$|\gamma - i|^2 \leq 16\epsilon \quad (57)$$

$$|\phi - i|^2 \leq 16\epsilon. \quad (58)$$

Proof. From the discussion at the beginning of this section, we know that the probability that J passes the GHZ test is given by

$$\begin{aligned} \frac{1}{2} &+ \operatorname{Re} \left[\overline{c_{111}} \cdot c_{000} \left(\frac{-1 + \lambda\gamma + \gamma\phi + \phi\lambda}{4} \right) \right] \\ &+ \operatorname{Re} \left[\overline{c_{110}} \cdot c_{001} \left(\frac{-1 + \lambda\gamma + \gamma\bar{\phi} + \bar{\phi}\lambda}{4} \right) \right] \\ &+ \operatorname{Re} \left[\overline{c_{101}} \cdot c_{010} \left(\frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\phi + \phi\lambda}{4} \right) \right] \\ &+ \operatorname{Re} \left[\overline{c_{100}} \cdot c_{011} \left(\frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\bar{\phi} + \bar{\phi}\lambda}{4} \right) \right] \end{aligned} \quad (59)$$

Therefore, the quantity $(1 - \epsilon)$ satisfies

$$\begin{aligned} 1 - \epsilon &\leq \frac{1}{2} + |c_{111}| |c_{000}| \left| \frac{-1 + \lambda\gamma + \gamma\phi + \phi\lambda}{4} \right| \\ &+ |c_{110}| |c_{001}| \left| \frac{-1 + \lambda\gamma + \gamma\bar{\phi} + \bar{\phi}\lambda}{4} \right| \\ &+ |c_{101}| |c_{010}| \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\phi + \phi\lambda}{4} \right| \\ &+ |c_{100}| |c_{011}| \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\bar{\phi} + \bar{\phi}\lambda}{4} \right| \end{aligned} \quad (60)$$

which implies

$$\begin{aligned} 1 - \epsilon &\leq \frac{1}{2} + \frac{1}{2} \left[\left(|c_{111}|^2 + |c_{000}|^2 \right) \left| \frac{-1 + \lambda\gamma + \gamma\phi + \phi\lambda}{4} \right| \right. \\ &+ \left(|c_{110}|^2 + |c_{001}|^2 \right) \left| \frac{-1 + \lambda\gamma + \gamma\bar{\phi} + \bar{\phi}\lambda}{4} \right| \\ &+ \left(|c_{101}|^2 + |c_{010}|^2 \right) \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\phi + \phi\lambda}{4} \right| \\ &\left. + \left(|c_{100}|^2 + |c_{011}|^2 \right) \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\bar{\phi} + \bar{\phi}\lambda}{4} \right| \right], \end{aligned} \quad (61)$$

or equivalently,

$$\begin{aligned}
1 - 2\epsilon &\leq \left(|c_{111}|^2 + |c_{000}|^2 \right) \left| \frac{-1 + \lambda\gamma + \gamma\phi + \phi\lambda}{4} \right| \\
&+ \left(|c_{110}|^2 + |c_{001}|^2 \right) \left| \frac{-1 + \lambda\gamma + \gamma\bar{\phi} + \bar{\phi}\lambda}{4} \right| \\
&+ \left(|c_{101}|^2 + |c_{010}|^2 \right) \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\phi + \phi\lambda}{4} \right| \\
&+ \left(|c_{100}|^2 + |c_{011}|^2 \right) \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\bar{\phi} + \bar{\phi}\lambda}{4} \right|.
\end{aligned} \tag{62}$$

Consider the following four quantities from inequality (62):

$$\left| \frac{-1 + \lambda\gamma + \gamma\phi + \phi\lambda}{4} \right|, \left| \frac{-1 + \lambda\gamma + \gamma\bar{\phi} + \bar{\phi}\lambda}{4} \right|, \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\phi + \phi\lambda}{4} \right|, \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\bar{\phi} + \bar{\phi}\lambda}{4} \right|.$$

Note that the coefficients of these quantities in (62) sum to 1. By Lemma B.2, the second, third, and fourth quantities are each less than or equal to $\sqrt{2}/2$. If the first of the quantities were also less than or equal to $\sqrt{2}/2$, then we have $1 - 2\epsilon \leq \frac{\sqrt{2}}{2}$, and therefore $\epsilon \geq \frac{1}{2} - \frac{\sqrt{2}}{4} > \frac{1}{8}$, and inequalities (56) - (58) would be trivially satisfied. So, let us assume that the first of these quantities is greater than $\sqrt{2}/2$, which makes it the largest of the four. Then,

$$1 - 2\epsilon \leq \left| \frac{-1 + \lambda\gamma + \gamma\phi + \phi\lambda}{4} \right|. \tag{63}$$

By Lemma B.1,

$$1 - 2\epsilon \leq \sqrt{1 - \frac{|\lambda - i|^2}{4}}. \tag{64}$$

Therefore,

$$(1 - 2\epsilon)^2 \leq 1 - \frac{|\lambda - i|^2}{4} \tag{65}$$

$$1 - 4\epsilon \leq 1 - \frac{|\lambda - i|^2}{4} \tag{66}$$

$$16\epsilon \geq |\lambda - i|^2 \tag{67}$$

Similar reasoning shows that $|\gamma - i|^2 \leq 16\epsilon$ and $|\phi - i|^2 \leq 16\epsilon$. \square

Proposition B.5. *Let J be the device from Proposition B.4. Let*

$$g = \frac{1}{\sqrt{2}} (|000\rangle - |111\rangle) \tag{68}$$

Then,

$$|\langle \alpha, g \rangle| \geq 1 - 7\epsilon. \tag{69}$$

Proof. As before, we know that the probability that the probability that J passes the GHZ test is given by (59). We prove the proposition in 3 cases.

Case 1: $\mathbf{c}_{000} = \mathbf{c}_{111} = \mathbf{0}$.

Using Lemma B.2, we have the following:

$$1 - \epsilon = \frac{1}{2} + \operatorname{Re} \left[\overline{c_{110}} \cdot c_{001} \left(\frac{-1 + \lambda\gamma + \gamma\bar{\phi} + \bar{\phi}\lambda}{4} \right) \right] \quad (70)$$

$$\begin{aligned} &+ \operatorname{Re} \left[\overline{c_{101}} \cdot c_{010} \left(\frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\phi + \phi\lambda}{4} \right) \right] \\ &+ \operatorname{Re} \left[\overline{c_{100}} \cdot c_{011} \left(\frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\bar{\phi} + \bar{\phi}\lambda}{4} \right) \right] \\ &\leq \frac{1}{2} + |c_{110}| |c_{001}| \left| \frac{-1 + \lambda\gamma + \gamma\bar{\phi} + \bar{\phi}\lambda}{4} \right| \\ &\quad + |c_{101}| |c_{010}| \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\phi + \phi\lambda}{4} \right| \\ &\quad + |c_{100}| |c_{011}| \left| \frac{-1 + \lambda\bar{\gamma} + \bar{\gamma}\bar{\phi} + \bar{\phi}\lambda}{4} \right| \end{aligned} \quad (71)$$

$$\begin{aligned} &\leq \frac{1}{2} + \left(\frac{|c_{110}|^2 + |c_{001}|^2}{2} \right) \cdot \frac{\sqrt{2}}{2} \\ &\quad + \left(\frac{|c_{101}|^2 + |c_{010}|^2}{2} \right) \cdot \frac{\sqrt{2}}{2} \\ &\quad + \left(\frac{|c_{100}|^2 + |c_{011}|^2}{2} \right) \cdot \frac{\sqrt{2}}{2} \\ &= \frac{1}{2} + \frac{\sqrt{2}}{4} \end{aligned} \quad (72)$$

Therefore,

$$\epsilon \geq 1 - \left(\frac{1}{2} + \frac{\sqrt{2}}{4} \right) \quad (73)$$

Since the quantity above is greater than $\frac{1}{7}$, condition (69) is trivially satisfied.

Case 2: $\mathbf{c}_{001} = \mathbf{c}_{010} = \mathbf{c}_{100} = \mathbf{c}_{011} = \mathbf{c}_{101} = \mathbf{c}_{110} = \mathbf{0}$.

We have

$$\begin{aligned}
1 - \epsilon &= \frac{1}{2} + \operatorname{Re} \left[\overline{c_{111}} \cdot c_{000} \left(\frac{-1 + \lambda\gamma + \gamma\phi + \phi\lambda}{4} \right) \right] \\
&= \operatorname{Re} \left[\overline{c_{111}} \cdot c_{000} \left(\frac{-1}{4} \right) \right] + \operatorname{Re} \left[\overline{c_{111}} \cdot c_{000} \left(\frac{\lambda\gamma + \gamma\phi + \phi\lambda}{4} \right) \right] \\
&\leq \operatorname{Re} \left[\overline{c_{111}} \cdot c_{000} \left(\frac{-1}{4} \right) \right] + |c_{111}| |c_{000}| \left| \frac{\lambda\gamma + \gamma\phi + \phi\lambda}{4} \right| \\
&\leq \operatorname{Re} \left[\overline{c_{111}} \cdot c_{000} \left(\frac{-1}{4} \right) \right] + \left(\frac{|c_{111}|^2 + |c_{000}|^2}{2} \right) \left| \frac{\lambda\gamma + \gamma\phi + \phi\lambda}{4} \right| \\
&\leq \operatorname{Re} \left[\overline{c_{111}} \cdot c_{000} \left(\frac{-1}{4} \right) \right] + \left(\frac{1}{2} \right) \left(\frac{3}{4} \right)
\end{aligned}$$

which implies, by a linear manipulation,

$$1 - 8\epsilon \leq (-2) \cdot \operatorname{Re} [\overline{c_{111}} c_{000}] \quad (74)$$

We have the following:

$$2 - 8\epsilon \leq 1 - 2 \cdot \operatorname{Re} [\overline{c_{111}} c_{000}] \quad (75)$$

By an easy calculation, the right side of this inequality is equal to $2|\langle \alpha, g \rangle|^2$. Thus,

$$2 - 8\epsilon \leq 2|\langle \alpha, g \rangle|^2 \quad (76)$$

$$1 - 4\epsilon \leq |\langle \alpha, g \rangle|^2 \quad (77)$$

$$1 - 4\epsilon \leq |\langle \alpha, g \rangle| \quad (78)$$

$$1 - 7\epsilon \leq |\langle \alpha, g \rangle|. \quad (79)$$

Case 3: General case.

Let

$$\alpha = x\alpha' + y\alpha'' \quad (80)$$

where α', α'' are unit vectors satisfying the conditions of Case 1 and Case 2, respectively, and (x, y) is a unit-length vector in \mathbb{R}^2 . Let $J_{\alpha'}$ and $J_{\alpha''}$ denote the device J with the state α replaced by α' and α'' , respectively. It is clear from expression (59) that

$$\begin{aligned}
\mathbf{P}(J \text{ passes the GHZ test}) &= x^2 \cdot \mathbf{P}(J_{\alpha'} \text{ passes the GHZ test}) \\
&+ y^2 \cdot \mathbf{P}(J_{\alpha''} \text{ passes the GHZ test}).
\end{aligned}$$

This case follows from cases 1 and 2 by an easy linearity argument. \square

Corollary B.6. *Let J be the device from Proposition B.4. There exists a complex number ζ with $|\zeta| = 1$ such that*

$$\|\alpha - \zeta g\|^2 \leq 14\epsilon. \quad (81)$$

Proof. Choose ζ so that the inner product $\langle \alpha, \zeta g \rangle$ is a nonnegative real number. (Thus, $\langle \alpha, \zeta g \rangle = |\langle \alpha, g \rangle|$.) Then,

$$\|\alpha - \zeta g\|^2 = \langle \alpha, \alpha \rangle - \langle \alpha, \zeta g \rangle - \langle \zeta g, \alpha \rangle + \langle \zeta g, \zeta g \rangle \quad (82)$$

$$= 2 - 2|\langle \alpha, g \rangle| \quad (83)$$

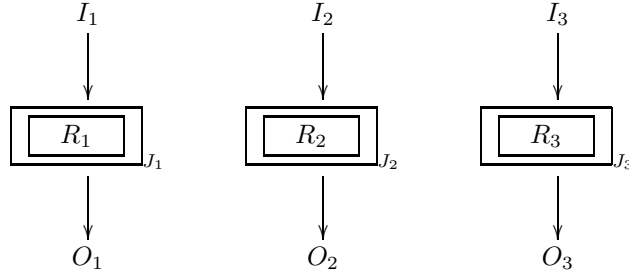
$$\leq 2 - 2(1 - 7\epsilon) \quad (84)$$

$$= 14\epsilon. \quad (85)$$

□

B.3 The Post-Measurement State of an Approximate GHZ Device

Let J be the 3-part RE device from Proposition B.4. Suppose, as usual, that J is given an input string $I_1 I_2 I_3$ that is randomly chosen from the set $\{000, 011, 101, 110\}$. Consider the post-measurement state of J together with its input and output registers.



Recall that the pre-measurement state of $R = (R_1, R_2, R_3)$ is a pure state α . We can express the post-measurement state of IOR as a pure state like so:

$$v_{IOR}^{(post)} = \left[\left(\frac{1}{4} \right) \cdot \sum_{(i_k), (o_k)} |i_1 i_2 i_3\rangle \otimes |o_1 o_2 o_3\rangle \otimes \left(\frac{\mathbb{I} + (-1)^{o_1} S_1^{(i_1)}}{2} \right) \otimes \left(\frac{\mathbb{I} + (-1)^{o_2} S_2^{(i_2)}}{2} \right) \otimes \left(\frac{\mathbb{I} + (-1)^{o_3} S_3^{(i_3)}}{2} \right) \right] \alpha. \quad (86)$$

where the summation is taken over all input/output combinations (i_k) , (o_k) which satisfy the GHZ test ((1)–(2)).

Let

$$g = \frac{1}{\sqrt{2}} (|000\rangle - |111\rangle) \quad (87)$$

and

$$\sigma^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \sigma^{(1)} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \quad (88)$$

Define a new state, denoted $v_{IOR}^{(ideal)}$, by expression (86) with the operators $S_k^{(i)}$ replaced by $\sigma^{(i)}$ and the state α replaced by g :

$$\begin{aligned} v_{IOR}^{(ideal)} = & \left[\left(\frac{1}{4} \right) \cdot \sum_{(i_k), (o_k)} |i_1 i_2 i_3\rangle \otimes |o_1 o_2 o_3\rangle \otimes \right. \\ & \left. \left(\frac{\mathbb{I} + (-1)^{o_1} \sigma^{(i_1)}}{2} \right) \otimes \left(\frac{\mathbb{I} + (-1)^{o_2} \sigma^{(i_2)}}{2} \right) \otimes \left(\frac{\mathbb{I} + (-1)^{o_3} \sigma^{(i_3)}}{2} \right) \right] g. \end{aligned} \quad (89)$$

This is the post-measurement state of the ideal GHZ device from subsection B.2.

Let us compare expressions (86) and (89). From Proposition B.4, we have

$$\left\| S_k^{(i_k)} - \sigma^{(i_k)} \right\|_2^2 \leq 32\epsilon. \quad (90)$$

Therefore,

$$\left\| S_k^{(i_k)} - \sigma^{(i_k)} \right\|_\infty \leq \left\| S_k^{(i_k)} - \sigma^{(i_k)} \right\|_2 \quad (91)$$

$$\leq \sqrt{32\epsilon}. \quad (92)$$

The individual projection operators from (86) and (89) therefore satisfy

$$\left\| \left(\frac{\mathbb{I} + (-1)^{o_k} S_1^{(i_k)}}{2} \right) - \left(\frac{\mathbb{I} + (-1)^{o_k} \sigma^{(i_k)}}{2} \right) \right\|_\infty \leq \frac{\sqrt{32\epsilon}}{2} = \sqrt{8\epsilon} \quad (93)$$

Let M and $M^{(ideal)}$ be the operators enclosed in brackets in (86) and (89), respectively. Applying Lemma B.3, we find that

$$\left\| M - M^{(ideal)} \right\|_\infty \leq 3 \cdot \sqrt{8\epsilon}. \quad (94)$$

By Corollary B.6, there is a unit-length complex number ζ such that

$$\|\alpha - \zeta g\|^2 \leq 14\epsilon. \quad (95)$$

Therefore:

$$\begin{aligned} \left\| v_{IOR}^{(post)} - \zeta \cdot v_{IOR}^{(ideal)} \right\| &= \left\| M\alpha - M^{(ideal)}(\zeta g) \right\| \\ &\leq \left\| M\alpha - M^{(ideal)}\alpha \right\| + \left\| M^{(ideal)}\alpha - M^{(ideal)}(\zeta g) \right\| \\ &\leq \left\| M - M^{(ideal)} \right\|_\infty + \|M\|_\infty \|\alpha - \zeta g\| \\ &\leq 3 \cdot \sqrt{8\epsilon} + \sqrt{14\epsilon}. \end{aligned}$$

Squaring, we find

$$\left\| v_{IOR}^{(post)} - \zeta \cdot v_{IOR}^{(ideal)} \right\|^2 \leq \left(3\sqrt{8} + \sqrt{14} \right)^2 \epsilon \quad (96)$$

$$< 150\epsilon. \quad (97)$$

We state the above inequality as a proposition.

Proposition B.7. *Let J be the device from Proposition B.4. Suppose that*

$$\mathbf{P}(J \text{ passes the GHZ test}) = 1 - \epsilon. \quad (98)$$

Then, there exists a unit-length complex number ζ such that

$$\left\| v_{IOR}^{(post)} - \zeta \cdot v_{IOR}^{(ideal)} \right\|^2 \leq 150\epsilon \quad (99)$$

where $v_{IOR}^{(ideal)}$ denotes the post-measurement state of the ideal GHZ device.

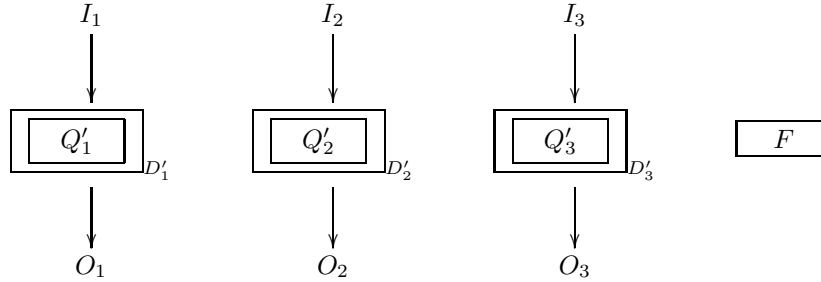
C The GHZ Paradox: General Case

Now we will broaden our focus and consider 3-part RE devices that contain arbitrarily large quantum systems.

C.1 The Post-Measurement State of an Approximate GHZ Device: General Case

As in subsection B.3, if R is a 3-qubit system, then we write $v_{IOR}^{(ideal)}$ for the post-measurement state of an ideal GHZ device on R . Also, we will write $\Gamma_{IOR}^{(ideal)}$ for the corresponding density operator.

Theorem C.1. *Let D' be a 3-part RE device that is in the canonical form described in Proposition A.1. Let F be a quantum system which is entangled with D' in such a way that the state $\Gamma_{Q'F}$ is pure. Let I and O denote the input and output registers of D' .*



Suppose that

$$\mathbf{P}(D' \text{ satisfies the GHZ paradox}) = 1 - \epsilon. \quad (100)$$

Then, there exists a unit vector

$$w \in \mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C} \otimes \mathcal{F} \quad (101)$$

such that the inequality

$$\left\| v_{IOQ'F}^{(post)} - w \otimes v_{IOR}^{(ideal)} \right\|^2 \leq 150\epsilon \quad (102)$$

holds.³

Proof. Choose an orthonormal basis $\{f_n\}$ for F . Let us write the pre-measurement state $v_{Q'F}^{(pre)}$ as

$$v_{Q'F}^{(pre)} = \sum_{klmn} (a_k \otimes b_l \otimes c_m \otimes f_n) \otimes \alpha_{klmn}. \quad (103)$$

with $\alpha_{klmn} \in \mathcal{R}_1 \otimes \mathcal{R}_2 \otimes \mathcal{R}_3$.

For every 4-tuple (k, l, m, n) which is such that $\alpha_{klmn} \neq 0$, define J_{klmn} to be the 3-part RE device on the system (R_1, R_2, R_3) whose pre-measurement state is

$$\frac{\alpha_{klmn}}{|\alpha_{klmn}|} \quad (104)$$

and whose measurement operators are given by

$$\begin{aligned} S_1^{(0)} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & S_2^{(0)} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & S_3^{(0)} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ S_1^{(1)} &= \begin{bmatrix} 0 & \lambda_k \\ \bar{\lambda}_k & 0 \end{bmatrix} & S_2^{(1)} &= \begin{bmatrix} 0 & \gamma_l \\ \bar{\gamma}_l & 0 \end{bmatrix} & S_3^{(1)} &= \begin{bmatrix} 0 & \phi_m \\ \bar{\phi}_m & 0 \end{bmatrix} \end{aligned} \quad (105)$$

For each device J_{klmn} , choose a unit-length complex number ζ_{klmn} so as to minimize the Euclidean distance between $\zeta_{klmn} \cdot v_{IOR}^{(ideal)}$ and the post-measurement state of J_{klmn} . Let

$$w = \sum_{klmn} (a_k \otimes b_l \otimes c_m \otimes f_n) \otimes \zeta_{klmn} |\alpha_{klmn}|. \quad (106)$$

Note that

$$\mathbf{P}(D' \text{ passes the GHZ test}) = \sum_{klmn} |\alpha_{klmn}|^2 \mathbf{P}(J_{klmn} \text{ passes the GHZ test})$$

Likewise, we can express the quantity

$$\left\| v_{IOQ'F}^{(post)} - w \otimes v_{IOR}^{(ideal)} \right\|^2 \quad (107)$$

³Note that in expression (102), we have treated the vector spaces \mathcal{R}_j from the statement of Proposition A.1 as the state spaces of a 3-qubit system. The expression $v_{IOR}^{(ideal)}$ represents the post-measurement state of an ideal GHZ device on this system.

as a weighted sum of the squares of the distances between the vectors $\zeta_{klmn} \cdot v_{IOR}^{(ideal)}$ and the post-measurement states of J_{klmn} . Inequality (102) thus follows from Proposition B.7 by linearity. \square

Let us consider how Theorem C.1 may be strengthened. We wish to cover the case in which the stated device D' is entangled with another quantum system F_1 , but the state $\Gamma_{Q'F_1}^{(pre)}$ is not pure. In this case, we can simply introduce a second entangled quantum system F_2 such that $\Gamma_{Q'F_1F_2}^{(pre)}$ is pure. By the theorem, we find that for some vector w in the tensor product of \mathcal{A} , \mathcal{B} , \mathcal{C} , \mathcal{F}_1 , and \mathcal{F}_2 ,

$$\left\| v_{IOQ'F_1F_2}^{(post)} - w \otimes v_{IOR}^{(ideal)} \right\|^2 \leq 150\epsilon. \quad (108)$$

We would like a similar expression with the system F_2 omitted. Since we cannot use vector-length to measure distance in this case, we use the trace-norm instead.

$$\begin{aligned} \left\| \Gamma_{IOQ'F_1}^{(post)} - \text{Tr}_{\mathcal{F}_2} (ww^\dagger) \otimes \Gamma_{IOR}^{(ideal)} \right\|_1^2 &\leq \left\| \Gamma_{IOQ'F_1F_2}^{(post)} - ww^\dagger \otimes \Gamma_{IOR}^{(ideal)} \right\|_1^2 \\ &\leq \left(2 \left\| v_{IOQ'F_1F_2}^{(post)} - w \otimes v_{IOR}^{(ideal)} \right\| \right)^2 \\ &\leq 600\epsilon. \end{aligned}$$

We have the following alternate statement of the theorem.

Theorem C.2. *Let D' be a device which is in the canonical form described in Proposition A.1. Let F_1 be a quantum system which may be entangled (in a possibly mixed state) with D' . Suppose that D' passes the GHZ test with probability $1 - \epsilon$. Then, there exists a density operator Φ_{ABCF_1} on $\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C} \otimes \mathcal{F}_1$ such that*

$$\left\| \Gamma_{IOQ'F_1}^{(post)} - \Phi_{ABCF_1} \otimes \Gamma_{IOR}^{(ideal)} \right\|_1^2 \leq 600\epsilon. \quad (109)$$

Secondly, we would like to have a version of the theorem which applies to devices that are not in canonical form. To simplify matters, let us drop the quantum system Q' and all of its subsystems from (109). We have:

$$\left\| \Gamma_{IOF_1}^{(post)} - \Phi_{F_1} \otimes \Gamma_{IO}^{(ideal)} \right\|_1^2 \leq 600\epsilon \quad (110)$$

Since a unitary embedding of one entangled 3-part RE device into another obviously has no effect on the quantity in this inequality, we have the following by Proposition A.1.

Theorem C.3. *Let D be a 3-part RE device (not necessarily in canonical form) which passes the GHZ test with probability $1 - \epsilon$. Let E be a quantum system which may be entangled with D . Then, there exists a density operator Φ_E on \mathcal{E} such that*

$$\left\| \Gamma_{IOE}^{(post)} - \Phi_E \otimes \Gamma_{IO}^{(ideal)} \right\|_1^2 \leq 600\epsilon. \quad (111)$$

Finally, note that inequality (111) above implies

$$\|\Gamma_E - \Phi_E\|^2 \leq 600\epsilon. \quad (112)$$

Therefore,

$$\left\| \Gamma_E \otimes \Gamma_{IO}^{(ideal)} - \Phi_E \otimes \Gamma_{IO}^{(ideal)} \right\|_1^2 \leq 600\epsilon. \quad (113)$$

Applying the triangle inequality for $\|\cdot\|_1$, we find that

$$\left\| \Gamma_{IOE}^{(post)} - \Gamma_E \otimes \Gamma_{IO}^{(ideal)} \right\|_1^2 \leq 2400\epsilon. \quad (114)$$

We therefore have the following final version of our theorem.

Theorem C.4. *Let D be a 3-part RE device which passes the GHZ test with probability $1 - \epsilon$. Let E be a quantum system which may be entangled with D . Then,*

$$\left\| \Gamma_{IOE}^{(post)} - \Gamma_E \otimes \Gamma_{IO}^{(ideal)} \right\|_1^2 \leq 2400\epsilon. \quad (115)$$